IMPLEMENTASI IDS (INTRUSION DETECTION SYSTEM) DENGAN SNORT/SURICATA

Perancangan Keamanan Sistem dan Jaringan

Dosen Pengampu : Ferdi Cahyadi

Anggota Kelompok :

2201020098	Muhammad Rifqi
2201020123	Handicap
2201020139	Muhammad Iqbal Hordani
2201020101	Irsyad Widiansyah

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK DAN TEKNOLOGI KEMARITIMAN

UNIVERSITAS MARITIM RAJA ALI HAJI

2025/2026

BAB I

PENDAHULUAN

1. Latar Belakang

Seiring dengan meningkatnya kompleksitas dan ketergantungan sistem informasi terhadap jaringan komputer, keamanan jaringan menjadi isu yang sangat penting untuk dijaga. Ancaman siber seperti *port scanning*, *brute-force login*, serangan eksploitasi, dan upaya infiltrasi lainnya dapat menimbulkan dampak serius, termasuk gangguan layanan, pencurian data, dan kerusakan sistem. Penelitian terbaru menunjukkan bahwa penggunaan sistem *Intrusion Detection System* (IDS) menjadi salah satu mekanisme paling efektif dalam mendeteksi aktivitas berbahaya di jaringan secara real-time, terutama jika didukung oleh aturan (*rule*) yang tepat dan konfigurasi yang optimal. Menunjukkan bahwa IDS yang diimplementasikan dengan baik dapat mendeteksi serangan metaprogram eksploitasi melalui analisis paket jaringan, sehingga memberikan peringatan dini terhadap potensi ancaman.

Snort dan Suricata merupakan dua IDS open-source yang populer digunakan dalam skenario akademik maupun praktis karena kemampuan deteksi berbasis *signature* dan performanya dalam memonitor jaringan. Kemampuan Snort dan Suricata dalam mendeteksi aktivitas jaringan yang mencurigakan dianalisis, dan kedua sistem ini terbukti bahwa kedua IDS tersebut unggul dalam mendeteksi serangan aplikasi basis data seperti *SQL injection*, yang menegaskan peran penting IDS dalam melindungi layanan jaringan dari eksploitasi aplikasi. Snort dan Suricata menunjukkan bahwa meskipun keduanya sama-sama mampu mendeteksi ancaman jaringan, performa dan karakteristik deteksi masing-masing bisa berbeda tergantung pada konfigurasi dan beban jaringan. Suricata dinilai lebih tepat digunakan sebagai sistem deteksi intrusi karena memiliki akurasi yang tinggi serta kemampuan respons yang lebih cepat terhadap aktivitas jaringan. Dibandingkan Snort yang digunakan sebagai IPS, Suricata mampu memproses dan mengenali pola serangan dengan waktu respons yang lebih efisien, sehingga lebih mendukung

kebutuhan pemantauan jaringan secara real-time. Penggunaan IDS secara terintegrasi bersama teknologi lain seperti firewall dan visualisasi log dapat meningkatkan ketelitian pemantauan dan respons terhadap serangan, termasuk pola serangan kompleks dan *brute force attack*.

Dalam konteks pembelajaran dan penelitian, pemahaman mengenai implementasi IDS sangat penting karena bisa memahami bagaimana proses deteksi serangan berlangsung, bagaimana aturan IDS dibuat, serta bagaimana hasil log dianalisis. Lingkungan virtual seperti VirtualBox atau VMware sering dipilih untuk simulasi karena menyediakan ruang uji yang aman tanpa mengganggu jaringan nyata. Proyek ini bertujuan untuk mengimplementasikan kinerja IDS Suricata dalam mendeteksi serangan jaringan melalui simulasi *port scanning*, *ping flood*, dan *brute-force login*. Implementasi akan mencakup instalasi dan konfigurasi, pembuatan *custom rule* sederhana, serta analisis hasil deteksi yang diperoleh dalam bentuk file log.

2. Tujuan Proyek

1. Mengimplementasikan Intrusion Detection System (IDS) Suricata pada lingkungan jaringan virtual untuk memahami cara kerja masing-masing sistem dalam mendeteksi aktivitas mencurigakan.
2. Menguji kemampuan kedua IDS dalam mendeteksi berbagai jenis serangan yang disimulasikan, seperti *port scanning*, *ping flood*, dan *brute-force login*.
3. Menganalisis efektivitas deteksi berdasarkan log yang dihasilkan IDS Suricata untuk mengetahui perbedaan akurasi, kecepatan respons, serta jenis serangan yang dapat dideteksi.

3. Ruang Lingkup Pengerjaan

Ruang lingkup proyek ini meliputi:

- Instalasi dan konfigurasi Suricata pada sistem Ubuntu.
- Simulasi serangan jaringan (port scanning dengan Nmap, brute-force dengan Hydra, dan ping flood).
- Pembuatan *custom rules* untuk mendeteksi jenis serangan tertentu.
- Analisis log hasil deteksi.

- Evaluasi efektivitas IDS berdasarkan hasil pengujian.

BAB II

DASAR TEORI

1. Jaringan Komputer

Jaringan komputer dapat didefinisikan sebagai sebuah sistem terpadu yang terdiri dari sejumlah komputer dan perangkat pendukung lainnya yang saling terhubung dan bekerja sama untuk mewujudkan satu atau lebih tujuan bersama. Selain itu, jaringan ini juga berkaitan dengan proses pertukaran atau penyampaian informasi melalui berbagai titik sambungan (*nodes*) yang terangkai, baik menggunakan media kabel maupun nirkabel. Jaringan semacam ini umum dimanfaatkan oleh perangkat seperti komputer dan telepon untuk mengirimkan pesan melalui sistem internal masing-masing.

2. Keamanan Jaringan

Keamanan jaringan komputer menghadapi empat bentuk ancaman utama, yang pertama adalah Penyalahgunaan Informasi Internet of Things (IoT), yang timbul dari kebiasaan pengguna yang ceroboh mengklik atau mengunduh file, gambar, atau tautan yang berpotensi mengandung virus atau file tersembunyi, yang dapat menyebabkan kebocoran informasi atau infeksi komputer. Kedua adalah Penolakan Layanan Serangan Latar Belakang (DoS), di mana pengguna secara sengaja menunda atau memperlambat layanan jaringan secara ilegal, yang merusak keamanan jaringan komputer. Bentuk ancaman ketiga adalah Kerusakan pada Integritas Lingkungan Jaringan Komputer, yang dilakukan oleh peretas atau pihak tidak beretika yang menggunakan cara-cara ilegal untuk menghancurkan keamanan jaringan dan memengaruhi integritasnya. Terakhir, Kebocoran Informasi Komputer terjadi ketika informasi ditransmisikan langsung ke entitas yang tidak sah tanpa izin, dengan bentuk umum kerentanan seperti intrusi virus atau *Trojan horse*,

kerentanan sistem pengguna, penyadapan frekuensi gelombang radio, atau pemasangan peralatan pemantauan.

3. Intrusion Detection System (IDS)

Intrusion Detection System (IDS) merupakan sistem keamanan jaringan yang berfungsi untuk memantau, menganalisis, dan mendeteksi aktivitas mencurigakan dalam lalu lintas data jaringan. IDS bekerja dengan cara menginspeksi paket-paket data yang melintas dan membandingkannya dengan pola serangan yang sudah dikenal (signature-based) atau perilaku abnormal (anomaly-based). Tujuan utama IDS adalah memberikan peringatan dini kepada administrator jaringan apabila terjadi potensi pelanggaran keamanan, sehingga dapat dilakukan tindakan mitigasi sebelum serangan berkembang lebih jauh. Secara umum, IDS dapat ditempatkan pada jaringan atau host tertentu untuk mendeteksi upaya intrusi baik dari luar maupun dalam sistem. Dalam konteks proyek ini, IDS digunakan untuk mendeteksi aktivitas seperti port scanning, brute-force login, dan ping flood yang disimulasikan di lingkungan jaringan virtual, sehingga dapat memberikan gambaran nyata tentang bagaimana sistem deteksi intrusi bekerja dalam menjaga keamanan jaringan.

4. Suricata

Suricata merupakan sebuah sistem *Intrusion Detection and Prevention System* (IDS/IPS) bersifat *open-source* yang dikembangkan oleh Open Information Security Foundation (OISF). Sistem ini dirancang untuk memantau lalu lintas jaringan secara real-time serta mendeteksi berbagai jenis ancaman seperti serangan jaringan, anomali lalu lintas, dan eksploitasi terhadap layanan tertentu. Suricata mampu bekerja menggunakan *signature-based detection*, *protocol analysis*, serta deteksi berbasis anomali, sehingga memberikan kemampuan deteksi yang komprehensif terhadap aktivitas mencurigakan.

Selain itu, Suricata mendukung pemrosesan multi-threading yang memungkinkan analisis data jaringan dalam jumlah besar secara efisien. Ia juga kompatibel dengan rule milik Snort dan dapat menghasilkan log dalam berbagai format, termasuk JSON, yang memudahkan integrasi dengan sistem analitik seperti ELK Stack (Elasticsearch, Logstash, dan Kibana). Dalam implementasi proyek ini,

Suricata digunakan sebagai IDS untuk mengamati aktivitas jaringan, mendeteksi serangan seperti *ping flood*, *port scanning*, dan *brute-force login*, serta menghasilkan log yang menjadi dasar dalam proses analisis keamanan.

5. Nmap

Nmap atau *Network Mapper* merupakan alat pemindai jaringan berbasis *open-source* yang digunakan secara luas untuk melakukan eksplorasi dan audit keamanan jaringan. Nmap berfungsi mengidentifikasi perangkat yang terhubung dalam suatu jaringan, port yang terbuka, serta layanan yang aktif pada setiap port tersebut. Dengan menggunakan Nmap, pengguna dapat memperoleh informasi penting mengenai sistem target, seperti versi layanan dan sistem operasi yang digunakan, sehingga alat ini sangat berguna untuk pengujian penetrasi maupun analisis keamanan jaringan. Dalam konteks proyek ini, Nmap digunakan untuk mensimulasikan aktivitas port scanning yang umum dilakukan oleh penyerang. Proses scanning dilakukan dengan berbagai teknik seperti *SYN scan* dan *aggressive scan*, yang kemudian diamati oleh IDS Suricata untuk memastikan apakah aktivitas tersebut dapat terdeteksi dengan baik.

6. Hydra

Hydra merupakan salah satu alat keamanan jaringan berbasis *open source* yang dirancang untuk melakukan serangan *brute force* terhadap berbagai layanan jaringan seperti SSH, FTP, HTTP, dan RDP. Tool ini bekerja dengan mencoba berbagai kombinasi username dan password secara otomatis untuk mendapatkan kredensial yang valid dan memperoleh akses ke sistem target. Dalam konteks penelitian ini, Hydra digunakan untuk mensimulasikan serangan *brute force* login terhadap layanan SSH pada mesin korban. Penggunaan Hydra memungkinkan pengujian efektivitas IDS Suricata dalam mendeteksi aktivitas login berulang dari satu sumber yang sama dalam waktu singkat, yang merupakan pola khas serangan *brute force*.

Melalui pengujian ini, diperoleh pemahaman tentang bagaimana Suricata mengenali karakteristik lalu lintas mencurigakan yang dihasilkan oleh Hydra, seperti banyaknya percobaan koneksi TCP berturut-turut menuju port 22. Hasilnya

menunjukkan bahwa Suricata mampu memunculkan peringatan ketika mendeteksi upaya login berulang, membuktikan bahwa sistem IDS dapat bekerja secara efektif dalam mengidentifikasi ancaman berbasis autentikasi yang tidak sah.

BAB III

PERANCANGAN SISTEM / ARSITEKTUR

Sistem yang dikembangkan dalam proyek ini terdiri dari dua mesin virtual (VM) yang dijalankan menggunakan Oracle VirtualBox, membentuk lingkungan simulasi jaringan lokal (virtual network) yang merepresentasikan skenario serangan aktif terhadap server dan proses deteksi oleh sistem Intrusion Detection System (IDS) berbasis Suricata. Topologi ini dirancang untuk mensimulasikan berbagai jenis serangan jaringan termasuk *port scanning*, *brute-force login SSH*, dan *ping flood* serta untuk menguji efektivitas rule Suricata dalam mendeteksi aktivitas berbahaya.

Setiap mesin virtual dikonfigurasi dengan satu *interface network* bertipe Host-Only Adapter yang digunakan untuk komunikasi antar mesin dalam jaringan terisolasi tanpa akses ke internet. Penggunaan *NAT* hanya diperlukan saat proses instalasi paket atau pembaruan sistem.

A. Attacker (Windows + Nmap & Hydra)
    1. Peran

       Mesin ini berfungsi sebagai penyerang, yang menghasilkan berbagai jenis lalu lintas serangan seperti port scan menggunakan Nmap dan brute force SSH menggunakan hydra
    2. Konfigurasi Interface

       Tipe : Host Only Adapter

       Nama Interface : enp0s8

Ip Address : 192.168.56.1/24

Koneksi : Langsung menuju Victim Server

3. Tujuan Operasional:
   - Menghasilkan lalu lintas jaringan berbahaya untuk menguji sensitivitas Suricata IDS
   - Menganalisis bagaimana IDS merespon pola koneksi berulang, scanning, dan serangan login

B. Victim (Ubuntu Server + Suricata IDS)

1. Peran

   Mesin ini berfungsi sebagai attacker atau penyerang, yang menghasilkan berbagai jenis lalu lintas serangan seperti port scan menggunakan Nmap dan brute-force SSH menggunakan Hydra.

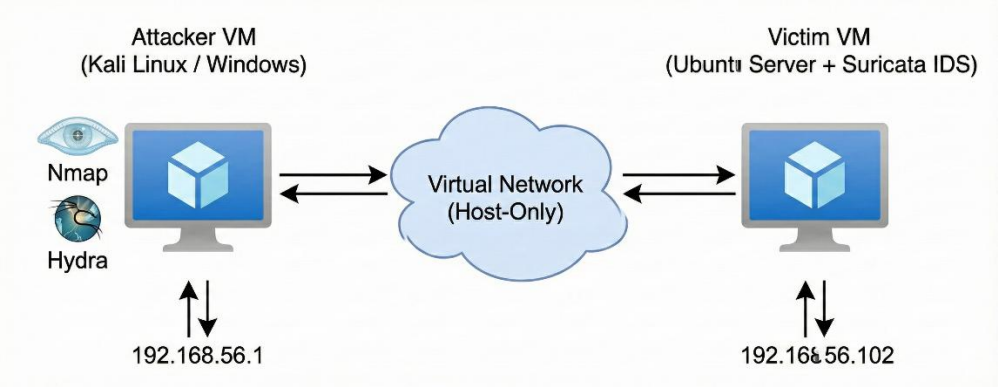
2. Konfigurasi Interface
   - Tipe : Host Only Adapter
   - Nama Interface : enp0s8
   - IP Address : 192.168.56.102/24
   - Koneksi : Menerima Koneksi dari attacker dan mencatat aktivitas menggunakan IDS Suricata
3. File Direktori
   - */etc/suricata/suricata.yaml,* untuk file konfig utama IDS
   - */etc/suricata/rules/local.rules,* sebagai tempat menyimpan custom rules yang dibuat sendiri
   - */var/log/suricata/fast.log* dan */var/log/suricata/eve.json,* Adalah log hasil deteksi IDS
4. Rule IDS yang Dirancang
   - alert tcp any any -> $HOME_NET 22 (msg:"[ALERT] Banyak Koneksi ke SSH - Kemungkinan brute-force"; flags:S; threshold:type both, track by_src, count 5, seconds 60; sid:1000004; rev:1;)

     Rule ini mendeteksi adanya banyak koneksi menuju port SSH (22) dalam waktu singkat, yang merupakan ciri serangan brute-force login.

- alert tcp any any -> $HOME_NET any (msg:"[SURICATA] Port Scan Terdeteksi"; flags:S; threshold:type threshold, track by_src, count 5, seconds 3; sid:1000001; rev:1;)

  Rule ini akan memicu alert apabila terdapat 5 koneksi SYN dalam waktu 3 detik dari satu sumber yang sama, yang biasanya mengindikasikan aktivitas port scanning.

C. Arsitektur Jaringan



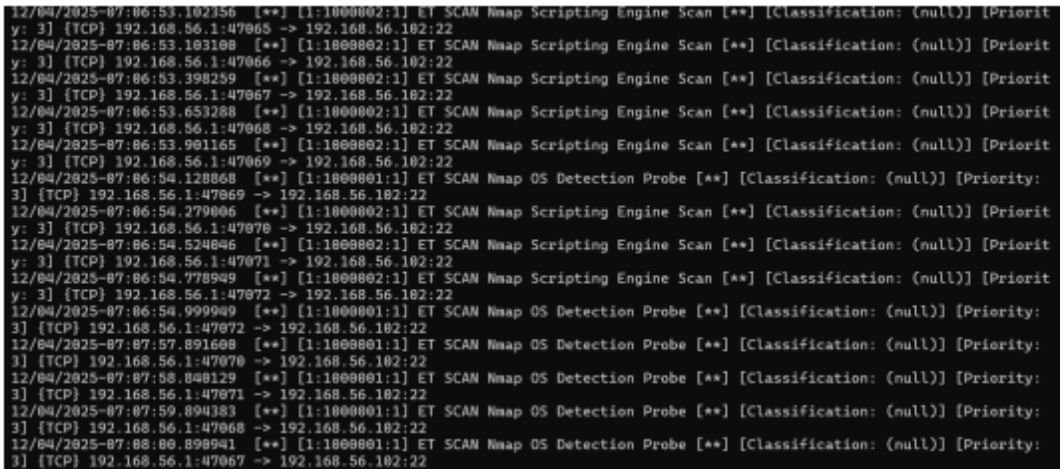
Jalur komunikasi ini memungkinkan lalu lintas langsung dari attacker menuju victim tanpa perantara router, sehingga Suricata dapat memantau semua paket yang masuk secara langsung di layer network.

D. Alur Komunikasi dan Deteksi

1. Serangan Port Scan Nmap

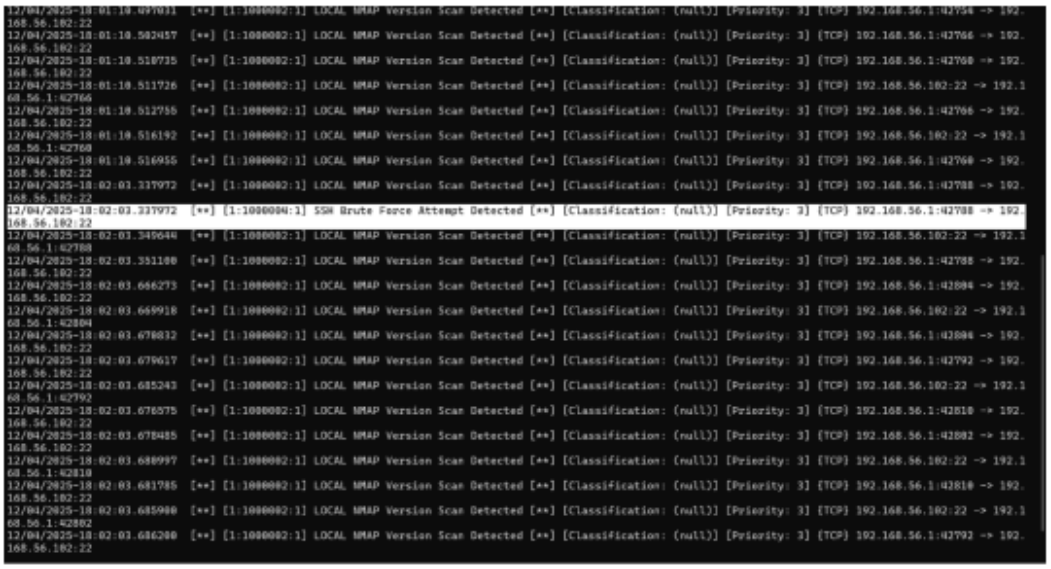
   - Attacker menjalankan perintah nmap -sS 192.168.56.102
   - Suricata mendeteksi pola SYN Scan dan menghasilkan alert:

```
ubuntu@ubuntuserver:~$ sudo tail -f /var/log/suricata/fast.log
12/04/2025-07:05:40.299555  [**] [1:1000003:1] ET SCAN Potential SYN Scan [**] [Classification: (null)] [Priority: 3] {T
CP} 192.168.56.1:63473 -> 192.168.56.102:139
12/04/2025-07:05:54.379186  [**] [1:1000003:1] ET SCAN Potential SYN Scan [**] [Classification: (null)] [Priority: 3] {T
CP} 192.168.56.1:62012 -> 192.168.56.102:554
```



- Ketika menggunakan mode nmap -A, Suricata juga mencatat aktivitas tambahan seperti:
    - ET SCAN Nmap Scripting Engine Scan
    - ET SCAN Nmap OS Detection Probe

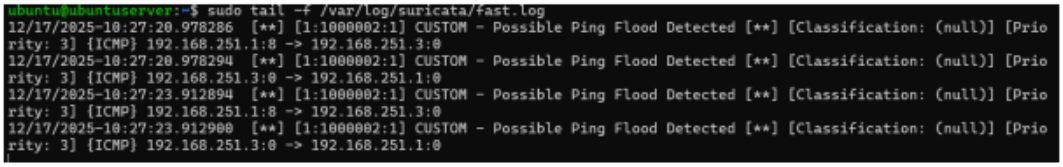
2. Serangan SSH Bruto Force Hydra
    - Attacker menjalankan hydra -l ubuntu -P passlist.txt ssh://192.168.56.102 -t 4.
    - Suricata mendeteksi 5 atau lebih percobaan login dalam waktu 60 detik.
    - Log deteksi:



([1:1000004:1] SSH Brute Force Attempt Detected {TCP} 192.168.56.1:42788 -> 192.168.56.102:22)

3. Serangan Ping Flood
    - Attacker mengirimkan ribuan paket ICMP secara cepat ke server.

- Suricata mengeluarkan alert:



BAB IV

IMPLEMENTASI

1. Konfigurasi Jaringan

Dalam implementasi proyek *Intrusion Detection System (IDS)* berbasis Suricata, dibutuhkan dua unit Virtual Machine (VM) untuk melakukan simulasi komunikasi antara mesin penyerang (attacker) dan mesin korban (victim).

Kedua VM ini dijalankan di atas platform Oracle VirtualBox, dan seluruh konfigurasi jaringan difokuskan pada jaringan internal (host-only) agar lalu lintas yang terjadi dapat dipantau dan dianalisis secara penuh oleh IDS.

Topologi sistem ini terdiri atas dua perangkat utama:

a. Mesin Attacker

   Kali Linux / Windows yang memiliki tools Nmap dan Hydra sebagai generator serangan.

b. Mesin Victim

   Ubuntu Server yang menjalankan Suricata IDS sebagai sistem pendeteksi serangan.

Keduanya terhubung melalui satu jaringan virtual dengan subnet 192.168.56.0/24, menggunakan interface yang sama (enp0s8) untuk komunikasi antar-VM.

Konfigurasi Jaringan VirtualBox:

Mesin	OS	Interface	IP Address	Fungsi
Attacker	Kali Linux / Windows	Enp0s8	192.168.56.1	Mengirim serangan berupa Nmap dan Hydra
Victim	Ubuntu Server dan Suricata	Enp0s8	192.168.56.102	Mendeteksi dan mencatat log serangan

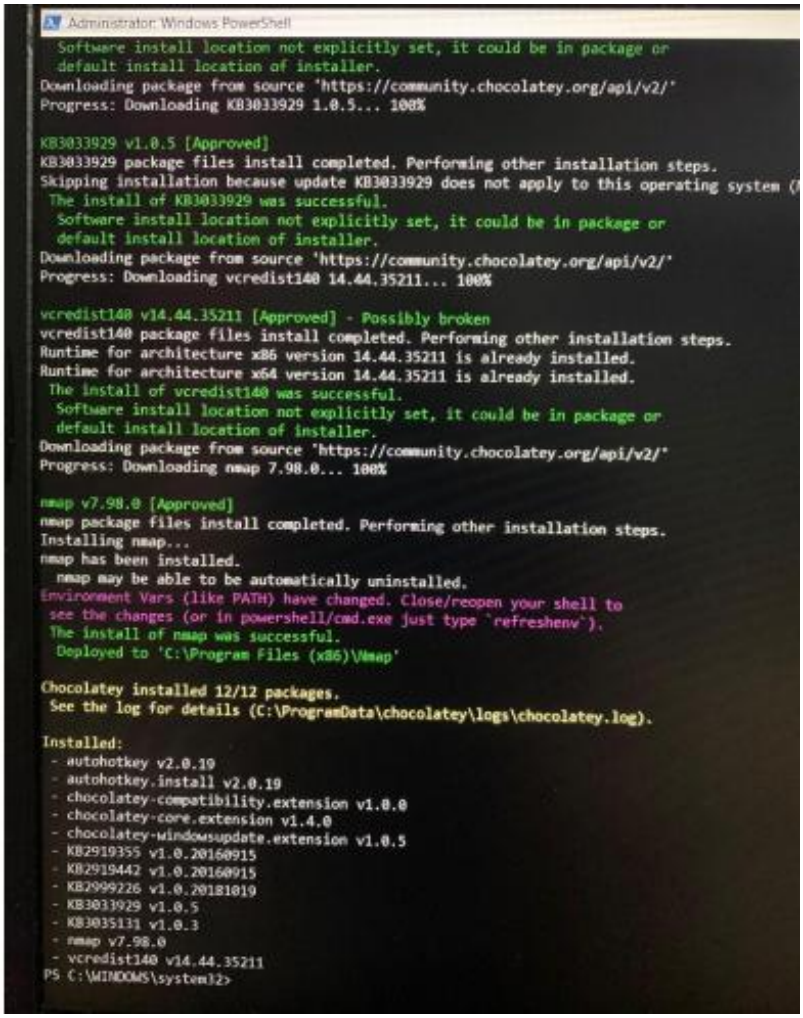
Setelah seluruh VM dikonfigurasi dan dijalankan, dilakukan pengujian konektivitas menggunakan perintah ping dari attacker ke victim. Hasilnya menunjukkan kedua mesin dapat saling berkomunikasi dengan lancar, menandakan bahwa jaringan LAN virtual telah terbentuk dengan benar.

2. Instalasi Software

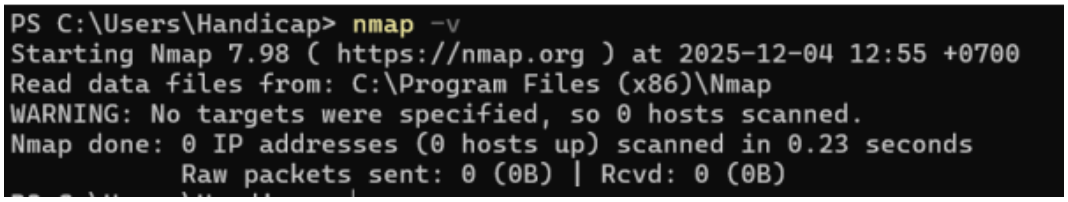
a. Mesin Attacker

i. Nmap

Digunakan untuk melakukan berbagai jenis pemindaian port pada server target, seperti Normal Scan, SYN Scan (-sS), dan Aggressive Scan (-A). Instalasi di windows:



choco install nmap



nmap -v

ii. Hydra

Digunakan untuk melakukan brute-force attack terhadap layanan SSH.

Instalasi di linux:

Sudo apt install hydra -y

Conoth perintah brute force:

Hydra -1 ubuntu -P passlist.txt ssh://192.168.56.102 -t 4

b. Mesin Victim

i. Suricata IDS

Berfungsi sebagai system deteksi serangan jaringan. Setelah instalasi, file konfigurasi utama (/etc/suricata/suricata.yaml) disesuaikan agar menggunakan interface enp0s8, serta dibuat direktori log:

```
sudo mkdir -p /var/log/suricata
sudo chmod 755 /var/log/suricata
sudo chown suricata:suricata /var/log/suricata
```

Kemudian dilakukan uji konfigurasi:

```
sudo suricata -T -c /etc/suricata/suricata.yaml -i enp0s8
```

ii. Pembuatan Custom File

File rule local diletakkan pada /etc/suricata/rules/local.rules dengan isi sebagai berikut:

```
alert tcp any any -> $HOME_NET any (flags:S; flow:stateless; msg:"CUSTOM - Possible TCP SYN Scan Detected"; threshold:type both, track by_src, count 10, seconds 5; sid:1001001; rev:1;)

alert udp any any -> $HOME_NET any (msg:"CUSTOM - Possible UDP Scan Detected"; flow:stateless; threshold:type both, track by_src, count 15, seconds 5; sid:1001003; rev:2;)

alert tcp any any -> $HOME_NET any (msg:"CUSTOM - Possible NULL Scan Detected (- sN)"; flags:0; flow:stateless; threshold:type both, track by_src, count 5, seconds 10; classtype:network-scan; sid:1003001; rev:1;)
```

BAB V

PENGUJIAN DAN ANALISIS

A. Simulasi Serangan Port Scanning Nmap

Pengujian ini dilakukan untuk mengidentifikasi kemampuan Suricata dalam mendeteksi aktivitas *port scanning*.

Attacker menjalankan perintah:

nmap -sS 192.168.56.102

```
PS C:\Users\Handicap> nmap -sS 192.168.56.102
Starting Nmap 7.98 ( https://nmap.org ) at 2025-12-04 14:05 +0700
Nmap scan report for 192.168.56.102 (192.168.56.102)
Host is up (0.0017s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 08:00:27:F3:C1:37 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
```

nmap 192.168.56.102

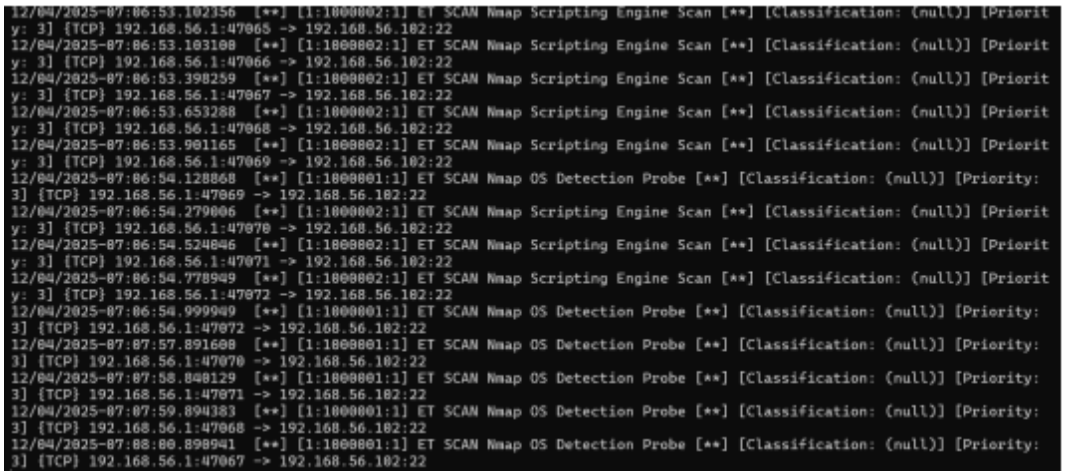
```
PS C:\Users\Handicap> nmap 192.168.56.102
Starting Nmap 7.98 ( https://nmap.org ) at 2025-12-04 13:58 +0700
Nmap scan report for 192.168.56.102 (192.168.56.102)
Host is up (0.0012s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 08:00:27:F3:C1:37 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
PS C:\Users\Handicap>
```

Hasil pengujian menunjukkan bahwa Suricata berhasil mendeteksi pola SYN Scan dan menghasilkan alert berikut di fast.log:

```
ubuntu@ubuntuserver:~$ sudo tail -f /var/log/suricata/fast.log
12/04/2025-07:05:40.299555  [**] [1:1000003:1] ET SCAN Potential SYN Scan [**] [Classification: (null)] [Priority: 3] {T
CP} 192.168.56.1:63473 -> 192.168.56.102:139
12/04/2025-07:05:54.379186  [**] [1:1000003:1] ET SCAN Potential SYN Scan [**] [Classification: (null)] [Priority: 3] {T
CP} 192.168.56.1:62012 -> 192.168.56.102:554
```

Pada mode *Aggressive Scan (-A)*, muncul alert tambahan:



Hal ini membuktikan bahwa Suricata mampu mengenali aktivitas scanning dari berbagai metode Nmap.

B. Simulasi Serangan SSH Brute Force Hydra

Attacker menggunakan Hydra untuk mencoba berbagai kombinasi password ke layanan SSH server dengan perintah:

hydra -l ubuntu -P passlist.txt ssh://192.168.56.102 -t 4

Hasil pada fast.log:

[1:1000004:1] SSH Brute Force Attempt Detected {TCP}

192.168.56.1:42788 → 192.168.56.102:22

Classtype: attempted-admin

Priority: 1 (High)

Suricata berhasil mendeteksi adanya ≥5 koneksi login dalam 60 detik dari sumber yang sama, menunjukkan bahwa mekanisme threshold rule bekerja sesuai konfigurasi.

C. SImulasi Serangan Ping Flood ICMP Flood

Pada tahap ini, attacker mengirimkan ribuan paket ICMP dalam waktu singkat untuk membanjiri server.

Hasil deteksi oleh Suricata:

CUSTOM - Possible Ping Flood Detected

Source: 192.168.56.1 → 192.168.56.102

Threshold: ≥1000 paket ICMP dalam 3 detik

Alert muncul berulang di file fast.log, menunjukkan bahwa IDS berhasil mendeteksi serangan *denial of service* ringan berbasis ICMP.

BAB VI

SARAN DAN KESIMPULAN

Berdasarkan hasil implementasi dan pengujian yang dilakukan, dapat disimpulkan bahwa sistem Intrusion Detection System (IDS) berbasis Suricata berhasil mendeteksi berbagai jenis serangan jaringan secara efektif, meliputi aktivitas *port scanning* menggunakan Nmap, serangan *brute-force login SSH* menggunakan Hydra, serta serangan *ping flood* berbasis ICMP. Setiap rule yang dirancang dan diimplementasikan pada file local.rules mampu menghasilkan alert sesuai dengan pola serangan yang dilakukan. Hasil log dari Suricata baik pada fast.log maupun eve.json menunjukkan bahwa IDS ini mampu memantau, mengenali, dan mengklasifikasikan lalu lintas mencurigakan dengan tingkat akurasi yang baik, menandakan bahwa sistem berjalan stabil dan konfigurasi yang diterapkan telah sesuai dengan tujuan penelitian.

Selain itu, penerapan custom rules pada tahap akhir terbukti meningkatkan sensitivitas sistem dalam mendeteksi pola serangan yang lebih spesifik dibanding rule bawaan. Lingkungan virtual yang dibangun menggunakan Oracle VirtualBox dengan dua mesin utama attacker dan victim berhasil mensimulasikan skenario serangan dan pertahanan jaringan secara realistis. Secara keseluruhan, implementasi ini menunjukkan bahwa Suricata IDS mampu berfungsi optimal dalam mendeteksi aktivitas serangan siber berbasis jaringan, serta dapat dijadikan dasar untuk pengembangan sistem keamanan jaringan yang lebih kompleks dan adaptif di masa mendatang.

Berikut ada bebrapa saran yang perlu dilakukan:

1. Optimasi rules tehreshold

   Untuk pengembangan berikutnya, perlu dilakukan penyesuaian parameter threshold agar dapat membedakan aktivitas normal (false positive) dengan serangan nyata. Misalnya, memperpanjang waktu interval atau menaikkan jumlah paket agar IDS tidak terlalu sensitif terhadap lalu lintas sah.
2. Integrasi dengan SIEM atau dashboard Analitik

   Hasil log Suricata dapat diintegrasikan dengan sistem Security Information and Event Management (SIEM) seperti ELK Stack (Elasticsearch, Logstash, Kibana) agar analisis log menjadi lebih interaktif, visual, dan real-time.
3. Implementasi Mode IPS

   Suricata tidak hanya dapat berfungsi sebagai IDS, tetapi juga dapat dikonfigurasi sebagai IPS yang mampu memblokir paket mencurigakan secara langsung. Penelitian lanjutan disarankan untuk mengevaluasi efektivitas mode pencegahan ini.

DAFTAR PUSTAKA

S. Alfarisy, E. S. Wijaya, & M. F. Noor. (2025). *Network Security Analysis with Hybrid Intrusion Detection System, Firewall, and Attacker Log Visualisation*. Jurnal Teknologi Informasi ULM.

https://jtiulm.ti.ft.ulm.ac.id/index.php/jtiulm/article/download/462/129

M. Syani. (2020). *Implementasi Intrusion Detection System (IDS) Menggunakan Suricata Pada Linux Debian 9 Berbasis Cloud Virtual Private Servers (VPS)*. Jurnal Inkofar.

https://www.researchgate.net/publication/349190055_IMPLEMENTASI_INTRUSION_DETECTION_SYSTEM_IDS_MENGGUNAKAN_SURICATA_PADA_LINUX_DEBIAN_9_BERBASIS_CLOUD_VIRTUAL_PRIVATE_SERVERS_VPS

D. B. Sufardy & I. R. Widiasari. (2024). *The Use of PFSense and Suricata as a Network Security Attack Detection and Prevention Tool on Web Servers*. INOVTEK Polbeng - Seri Informatika.

https://jurnal.polbeng.ac.id/index.php/ISI/article/download/159/33

E. Albin. (2011). *A Comparative Analysis of the Snort and Suricata Intrusion Detection Systems*. Defense Technical Information Center (DTIC).

https://apps.dtic.mil/sti/tr/pdf/ADA552115.pdf

S. Alharbi & A. Khan. (2023). *Ensemble Defense System: A Hybrid IDS Approach for Effective Cyber Threat Detection*. IEEE International Conference on Computer Networks and Applications.

https://arxiv.org/pdf/2401.03491

H. A. Damanik & M. Anggraeni. (2024). *Sistem Deteksi Intrusi Hybrid dan Mitigasi Kerentanan Infrastruktur Jaringan Menggunakan Teknik Active Response (XDR) Wazuh dan Suricata*. Jurnal Pekommas.

https://jkd.komdigi.go.id/index.php/pekommas/article/view/5829/2083

M. Hänninen. (2019). *Open Source Intrusion Detection Systems Evaluation for Small and Medium-Sized Enterprise Environments*. Theseus.fi.

https://www.theseus.fi/bitstream/handle/10024/265554/Markku%20H%C3%A4nninen%20thesis.pdf

D. Zielinski & H. A. Kholidy. (2022). *An Analysis of Honeypots and Their Impact as a Cyber Deception Tactic*. arXiv preprint arXiv:2301.00045.

https://arxiv.org/pdf/2301.00045